

| Module Name  | Imports      | OFTs     | TimeDateStamp | ForwarderChain | Name RVA | FTs (IAT) |
|--------------|--------------|----------|---------------|----------------|----------|-----------|
| 00012AA4     | N/A          | 00011FE4 | 00011FE8      | 00011FEC       | 00011FF0 | 00011FF4  |
| szAnsi       | (nFunctions) | Dword    | Dword         |                | Dword    | Dword     |
| SHELL32.dll  | 1            | 00012CA8 | FFFFFFFF      | FFFFFFFF       | 00012E42 | 0000109C  |
| msvcrt.dll   | 26           | 00012DC8 | FFFFFFFF      | FFFFFFFF       | 00012F60 | 000011BC  |
| ADVAPI32.dll | 3            | 00012C0C | FFFFFFFF      | FFFFFFFF       | 00012FFC | 00001000  |
| KERNEL32.dll | 30           | 00012C2C | FFFFFFFF      | FFFFFFFF       | 000131D4 | 00001020  |
| GDI32.dll    | 3            | 00012C1C | FFFFFFFF      | FFFFFFFF       | 0001320C | 00001010  |
| USER32.dll   | 69           | 00012CB0 | FFFFFFFF      | FFFFFFFF       | 000136A4 | 000010A4  |

  

| OFTs     | FTs (IAT) | Hint | Name            |
|----------|-----------|------|-----------------|
| Dword    | Dword     | Word | szAnsi          |
| 0001335C | 77D4BC10  | 012C | GetMenu         |
| 00013694 | 77D62697  | 0252 | SetDlgItemInt   |
| 00013682 | 77D3A331  | 017A | GetWindowTextW  |
| 00013670 | 77D3FF4A  | 0038 | CheckDlgButton  |
| 00013664 | 77D3817F  | 017F | HideCaret       |
| 00013652 | 77D3741F  | 001C | CallWindowProcW |
| 00013646 | 77D376C3  | 00BF | DrawTextW       |
| 0001363A | 77D5B765  | 02D3 | WinHelpW        |
| 00012670 | 77D3D816  | 0201 | PostQuitMessage |

**Import Directory**, vengono mostrati i moduli o le librerie (DLL) che questo eseguibile importa.

**SHLWAPI.dll** è una libreria di sistema di Windows, il cui nome sta per **Shell Lightweight Utility Library**. È utilizzata principalmente per fornire funzioni utili per la gestione di operazioni comuni nei programmi che interagiscono con il sistema operativo, in particolare con il file system e la shell di Windows (l'interfaccia grafica).

Alcune delle funzionalità offerte da **SHLWAPI.dll** includono:

1. **Gestione stringhe**: funzioni per la manipolazione delle stringhe di testo, come concatenazione, ricerca e formattazione.
2. **Operazioni su URL**: strumenti per l'analisi, combinazione e manipolazione degli URL.
3. **Interazione con il registro di sistema**: funzioni per leggere, scrivere e gestire chiavi del registro di Windows.
4. **Funzioni di confronto e ricerca**: utili per confrontare file o identificare tipi di dati.

Questa libreria è spesso utilizzata da applicazioni di Windows per eseguire operazioni di utilità legate alla gestione di file, URL e stringhe, riducendo la necessità per gli sviluppatori di implementare queste funzionalità da zero.

**msvcrt.dll (Microsoft Visual C Runtime Library)**: Questa DLL contiene le funzioni runtime della libreria C di Microsoft, utilizzate per fornire funzioni di base come la gestione di memoria,

I/O (input/output), la gestione di stringhe, funzioni matematiche e altro. È utilizzata da molte applicazioni sviluppate con Visual C++.

**ADVAPI32.dll (Advanced API Library):** Fornisce un insieme di API avanzate per Windows, utilizzate per funzioni legate alla sicurezza, gestione del registro di sistema, gestione dei servizi e altre funzionalità di basso livello relative all'amministrazione e alla sicurezza del sistema operativo.

**KERNEL32.dll (Windows Kernel API Library):** Questa libreria contiene la maggior parte delle funzioni di base del sistema operativo Windows, incluse la gestione della memoria, gestione dei processi e dei thread, gestione dell'I/O, operazioni su file e altro. È una delle DLL fondamentali per il funzionamento di Windows.

**GDI32.dll (Graphics Device Interface):** Fornisce funzioni grafiche per Windows, consentendo alle applicazioni di disegnare su schermo o su altri dispositivi di output. Include operazioni per il disegno di linee, forme, testo e immagini. Viene utilizzata per la grafica bidimensionale nelle applicazioni.

**USER32.dll (Windows User Interface API):** Contiene le funzioni per gestire gli elementi dell'interfaccia utente, come finestre, bottoni, caselle di testo e altri controlli. Include anche funzioni per la gestione dei messaggi di Windows, l'interazione con tastiera e mouse e la gestione delle finestre.

**calcolatriceinnovativa.exe**

| Name    | Virtual Size | Virtual Address | Raw Size | Raw Address | Reloc Address | Linenumbers | Relocations N... | Linenumbers |
|---------|--------------|-----------------|----------|-------------|---------------|-------------|------------------|-------------|
| Byte[8] | Dword        | Dword           | Dword    | Dword       | Dword         | Dword       | Word             | Word        |
| .text   | 000126B0     | 00001000        | 00012800 | 00000400    | 00000000      | 00000000    | 0000             | 0000        |
| .data   | 0000101C     | 00014000        | 00000A00 | 00012C00    | 00000000      | 00000000    | 0000             | 0000        |
| .rsrc   | 00008A70     | 00016000        | 00008C00 | 00013600    | 00000000      | 00000000    | 0000             | 0000        |

  

| Offset   | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | A  | B  | C  | D  | E  | F  | Ascii                            |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----------------------------------|
| 00000000 | 4D | 5A | 90 | 00 | 03 | 00 | 00 | 00 | 04 | 00 | 00 | 00 | FF | FF | 00 | 00 | MZ . . . . . y . .               |
| 00000010 | B8 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 40 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | . . . . . @ . . . . .            |
| 00000020 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | . . . . . . . . . . .            |
| 00000030 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | F0 | 00 | 00 | . . . . . 8 . . . . .            |
| 00000040 | 0E | 1F | BA | 0E | 00 | B4 | 09 | CD | 21 | B8 | 01 | 4C | CD | 21 | 54 | 68 | 0 20 . ' I , I I Th              |
| 00000050 | 69 | 73 | 20 | 70 | 72 | 6F | 67 | 72 | 61 | 6D | 20 | 63 | 61 | 6E | 6E | 6F | is . program . canno             |
| 00000060 | 74 | 20 | 62 | 65 | 20 | 72 | 75 | 6E | 20 | 69 | 6E | 20 | 44 | 4F | 53 | 20 | t . be . run . in . DOS .        |
| 00000070 | 6D | 6F | 64 | 65 | 2E | 0D | 0D | 0A | 24 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | mode . . . . . s .               |
| 00000080 | 87 | 45 | 16 | 64 | C3 | 24 | 78 | 37 | C3 | 24 | 78 | 37 | C3 | 24 | 78 | 37 | ! E0 dA \$ x 7 A \$ x 7 A \$ x 7 |
| 00000090 | 39 | 07 | 38 | 37 | C6 | 24 | 78 | 37 | 19 | 07 | 64 | 37 | C8 | 24 | 78 | 37 | 90 87 A \$ x 7 0 0 d 7 E \$ x 7  |

- Name:** Il nome della sezione. Ci sono tre sezioni elencate:
  - .text: La sezione che contiene il codice eseguibile (le istruzioni della CPU).
  - .data: Contiene i dati statici e variabili globali utilizzate dal programma.
  - .rsrc: La sezione che contiene le risorse del programma (icone, immagini, stringhe di testo, ecc.).
- Virtual Size:** La dimensione virtuale della sezione in memoria. Indica quanto spazio occupa questa sezione quando viene caricata in memoria.
- Virtual Address:** L'indirizzo di memoria virtuale in cui la sezione sarà caricata quando il programma viene eseguito.
- Raw Size:** La dimensione effettiva della sezione nel file eseguibile.
- Raw Address:** L'indirizzo all'interno del file eseguibile dove la sezione inizia.
- Reloc Address e Reloc Number:** Indicano informazioni sulla riallocazione degli indirizzi, che sono necessari quando un modulo o DLL viene spostato in una posizione di memoria diversa da quella predefinita. In questo caso, non ci sono informazioni sulla riallocazione (valori a zero).

## Parte inferiore (Hex e Ascii):

Nella parte inferiore della finestra, puoi vedere il **Dump Hexadecimale** del file, ovvero una rappresentazione in formato esadecimale dei dati presenti nel file eseguibile. Ogni byte del file è rappresentato sia in forma esadecimale che in forma ASCII (a destra).

Il dump inizia con "MZ", che è la firma di un file eseguibile di Windows (indica che è un file in formato DOS/Windows PE). La parte in ASCII mostra un messaggio classico: **"This program**

**cannot be run in DOS mode"**, che appare nei file eseguibili di Windows per indicare che non possono essere eseguiti su vecchi sistemi DOS senza interfaccia grafica.